STATE of ARIZONA

Government Information Technology Agency	Statewide STANDARD	TITLE: Network Infrastructure
	P100-S101	Effective Date: February 21, 2002

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (A.R.S. § 41-3504(A (1))), including, the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

The purpose of this standard is to coordinate agency and State implementations of network components and their designs. It is also intended to encourage further deployment of open systems based on targeted network architectures that use common, proven, pervasive, and industry-wide standards.

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology PSPs within each Agency.

4. STANDARD

The following network standards provide for more effective sharing of common IT resources in addition to improving quality, usefulness, and efficiency of cross-agency applications and information throughout the State.

4.1. **Copper Network Cabling:** Shall be Category 5e Unshielded Twisted Pair (UTP).

- Category 5e UTP is certified to carry 100/1000 Mbps of data.
- Category 5e UTP is an IEEE standard and is an industry-wide standard structured cabling system.
- UTP shall be used unless specific issues exist, such as high EMI or long transport distances.
- All cabling installations shall to conform to applicable building codes, IEEE, EIA/TIA, and BICSI.

4.2. **Fiber Network Cabling:** Shall be either single-mode or multi-mode, depending on requirements.

- All fiber network cabling shall be open and industry-wide standard, as supported by IEEE.
- Fiber network cabling within a building may be multi-mode or single-mode. Multi-mode transmits Gigabit Ethernet a distance of approximately 220 meters (62.5/125 micron) to 550 meters (50/125 micron), depending on the specific fiber and the Ethernet port characteristics, maximum. Single-mode (8/125 micron) transmits Gigabit Ethernet up to a distance of approximately 5,000 meters, maximum.
- Fiber network cabling between buildings shall be single-mode, allowing Gigabit Ethernet (and above) transmission rates over greater distances.
- All cabling installations shall to conform to applicable building codes, IEEE, EIA/TIA, and BICSI.

4.3. **Wireless Network Connectivity**: Shall be compliant with IEEE 802.11x (LAN) and IEEE 802.16 (MAN) and shall use the 802.1x security standard.

- IEEE 802.11x provides relatively high-speed (11 Mbps and 54 Mbps) LAN links.
- IEEE 802.16 (approved December 2001) provides Metropolitan Area Networks with up to 66 GHz of performance.

4.4. **Logical Network Topology:** Shall be a star, although the physical network topology may be a star, ring, or mesh.

- Star, ring, and mesh topologies are specified to minimize the effect of connection failures between devices while easing the addition or removal of network devices.
- Star, ring, and mesh topologies are both scalable and flexible.

4.5. **Network Link Layer Access Protocol:** Shall be Ethernet, IEEE 802.3, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method.

- Ethernet is scalable, with the newer, more recent versions able to manage the increase of data flow and provide the bandwidth and "end-to-end" Quality of Service (QoS) necessary to support the requirements of converged voice, data, and video applications.

4.6. **Transport and Network Protocols**: Shall be TCP/UDP and IP, respectively.

- TCP/UDP and IP make up an open protocol suite that allows Internet access and the seamless integration of Intranets, Extranets, VPNs, and LANs.
- TCP/UDP and IP protocols facilitate, simplify, and standardize the protocols used to deliver e-government services.

4.7. **Network Devices (routers, switches, firewalls, access servers, etc.):** Shall be manageable with Network Management platforms that use Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON).

- SNMP and RMON facilitate the exchange of management information between network devices as well as network performance management, isolation and analysis of network problems, and growth planning.
- SNMP is part of the TCP/IP protocol suite recommended for the transport and network protocol layers.
- Managed network devices help to ensure the continuous delivery of e-government services and internal agency business processes.

4.8. **Switching Technologies**: Shall be used to achieve Local Area Network (LAN) network device connectivity in OSI Layers 2, 3, and 4.

- Switching enhances security and network management. It improves network performance by enabling the balancing of network traffic across multiple segments, thus reducing resource contention, providing for scalability, and increasing throughput capacity.
- All communications over a LAN in Layers 2, 3, and 4 will use switching technologies.

4.9. **Network Interfaces**: Internal networks shall use "private," unregistered Internet Protocol (IP) addresses for network workstations and appliances. External networks communicating outside the agency shall use "public," registered IP addresses for all external ports on internetworking devices.

- Network Address Translation (NAT) techniques deployed at network boundaries to the external network or Internet enable the widespread reuse of non-unique or unregistered IPv4 addresses while still providing the required connectivity to applications and the external network or Internet.
- "Private," unregistered IP addresses provide additional security and protection of information and resources. NAT creates a firewall between the internal network and outside networks or the Internet by only allowing connections that originate inside the internal network.
- "Private," unregistered IP addresses provide flexibility and simplify the process of adding workstations and devices to networks.
- To prevent duplication and resulting loss of connectivity, the organization responsible for network administration shall coordinate all "private," unregistered IP addresses within their domain of responsibility.
- The Internet Assigned Numbers Authority (IANA) has reserved three blocks of IP address space for "private" Internets (Network Working Group RFC 1918). The blocks are 10.0.0.0. to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255. Any IP addresses outside of these spaces lack coordination with IANA or an Internet registry when used as unregistered IP addresses..
- "Public," registered IP addresses provide the required uniqueness for Internet and network integrity.
- IANA provides coordination of all "public" IP address space.

4.10. **Internal Workstation Network IP Addresses**: Shall be assigned using Dynamic Host Configuration Protocol (DHCP).

- DHCP provides the flexibility needed for growth and migration of networks.
- DHCP facilitates and simplifies IP network administration and the addition of workstations and devices to networks.
- DHCP address allocation may be (1) an automatic allocation where DHCP assigns a permanent IP address to the workstation; (2) manually allocated and assigned by the DHCP administrator; or (3) dynamically allocated where DHCP assigns an IP address to a workstation for a limited period of time (lease.)

5. DEFINITIONS AND ABBREVIATIONS

Refer to both, the PSP Glossary of Terms and the PSP Glossary of Abbreviations, for definitions and abbreviations.

6. REFERENCES

6.1. A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."
6.2. A. R. S. § 41-1335 ((A (6 & 7))),"State Agency Information."
6.3. A. R. S. § 41-1339 (A),"Depository of State Archives."
6.4. A. R. S. § 41-1461, "Definitions."
6.5. A. R. S. § 41-1463, "Discrimination; unlawful practices; definition".
6.6. A. R. S. § 41-1492 et seq., "Prohibition of Discrimination by Public Entities."
6.7. A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."
6.8. A. R. S. § 41-3501, "Definitions."
6.9. A. R. S. § 41-3504, "Powers and Duties of the Agency."
6.10. A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
6.11. A. R. S. § 44-7041, "Governmental Electronic Records."
6.12. Arizona Administrative Code, Title 2, Chapter 7, "Department of Administration Finance Division, Purchasing Office."
6.13. Arizona Administrative Code, Title 2, Chapter 10, "Department of Administration Risk Management Section."
6.14. Arizona Administrative Code, Title 2, Chapter 18, "Government Information Technology Agency."
6.15. Statewide Information Technology Policy P100.
6.16. Statewide IT Security Policy P800.
6.17. State of Arizona Target Network Architecture, http://gita.state.az.us/enterprise_architecture.

7. ATTACHMENTS

None.